ICS-CERT ADVISORY

ICSA-12-283-02—WELLINTECH KINGVIEW USER CREDENTIALS NOT SECURELY HASHED

October 9, 2012

OVERVIEW

This advisory is a follow-up to the alert titled ICS-ALERT-12-212-02—WellinTech KingView User Credentials Not Securely Hashed that was published July 30, 2012, on the ICS-CERT Web page.

Dr. Wesley McGrew of Mississippi State University has identified a default credential vulnerability in WellinTech KingView application. WellinTech has produced a patch that mitigates this vulnerability.

Exploits that target this vulnerability are known to be publicly available.

AFFECTED PRODUCTS

WellinTech reports that the vulnerability affects the following versions of KingView:

- KingView 6.5.3 and previous.

IMPACT

A successful exploit of this vulnerability will allow an attacker complete access of the targeted system.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

BACKGROUND

WellinTech is a software development company specializing in automation and control. WellinTech is based in Beijing, China, with branches in the United States, Japan, Singapore, Europe, and Taiwan.

According to the WellinTech Web site, the KingView product is a Windows-based control, monitoring, and data collection application deployed across several industries, including power, water, building automation, mining, and other sectors.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

USER CREDENTIALS NOT SECURELY HASHED[a]

KingView does not securely store user credentials. An attacker can decrypt the file containing usernames and passwords with a simple mathematical algorithm.

CVE-2012-4899[b] has been assigned to this vulnerability. A CVSS v2 base score of 6.8 has been assigned; the CVSS vector string is (AV:L/AC:L/Au:S/C:C/I:C/A:C).[c]

VULNERABILITY DETAILS

EXPLOITABILITY

An attacker needs to be able to access the system where the files are stored to exploit this vulnerability.

EXISTENCE OF EXPLOIT

Exploits that target this vulnerability are publicly available.

DIFFICULTY

An attacker with a low skill would be able to exploit this vulnerability.

MITIGATION

WellinTech has created a patch that fixes this vulnerability by increasing the complexity of the algorithm used to encrypt the passwords and usernames. A copy of the patch may be downloaded

a. CWE-311: Missing Encryption of Sensitive Data, http://cwe.mitre.org/data/definitions/311.html, Web site last accessed October 09, 2012.

b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4899, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

c. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:L/AC:L/Au:S/C:C/I:C/A:C), Web site last accessed October 09, 2012.

from the following location: http://www.wellintech.com/index.php/news/33-patch-for-kingview653.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT also provides a section for control systems security recommended practices on the US-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[d] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01A—Cyber Intrusion Mitigation Strategies,[e] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click Web links or open unsolicited attachments in email messages.
2. Refer to Recognizing and Avoiding Email Scams[f] for more information on avoiding email scams.
3. Refer to Avoiding Social Engineering and Phishing Attacks[g] for more information on social engineering attacks.

d. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed October 09, 2012.

e. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed October 09, 2012.

f. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, Web site last accessed October 09, 2012.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For industrial control systems security information and incident reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.

g. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, Web site last accessed October 09, 2012.